WHAT IS CLAIMED IS:

1. A method for on-line Personal Identification Number (PIN) verification comprising:

initializing a smart card with an entity-selected PIN hidden in a polynomial over a finite field, an initialization polynomial being a function of the PIN, an entity-identifier, and a random number; and

discarding the random number and the PIN after smart card initialization.

2. The method according to Claim 1 further comprising:

generating an ephemeral transaction polynomial using the smart card at an entity-activated terminal with an entity-entered PIN′ enabling recovery from a polynomial over a finite field, the ephemeral transaction polynomial being a function of the entity-entered PIN′, the entity-identifier, and a second random number;

sending a function of the ephemeral transaction polynomial and a difference between the second random number and a function of the PIN′ and the secret function to a host; and

discarding the second random number.

3. The method according to Claim 2 further comprising:

verifying that the PIN is equivalent to the PIN′ based on a relationship among the entity-identifier and a function of the initialization polynomial received from the on-line authorization system and the difference and function of the verification polynomial.

4. The method according to Claim 2 further comprising:

encrypting the function of the initialization polynomial prior to sending to the on-line authorization system; and

encrypting the function of the verification polynomial prior to sending to the host.

5. The method according to Claim 1 further comprising:

hiding the entity-selected PIN in a polynomial over a finite field of the form:

$$y = a_0 + \sum_{i=1}^{n} a_i x^i \,(\mathrm{mod}\, P),$$

where P is a large prime number.

6. The method according to Claim 1 further comprising:

receiving on the smart card a large prime integer P, an entity-identifier x, and the entity-selected PIN;

generating on the smart card a random number a_{ri} between a lower limit L and the large prime integer P;

computing a polynomial:

$$y_r = PIN + \sum_{i=1}^{N} a_{ri} \cdot x^i \,(\mathrm{mod}\, P);$$

encrypting value y_r as encryption function $E_k[y_r]$;

sending the encryption function $E_k[y_r]$ to the on-line authorization system;

computing on the smart card at least one value:

$z_i = PIN^{-1} \cdot a_{ri} (\mathrm{mod}\ P)$;

retaining the at least one value z_i on the smart card; and

erasing the random number a_r and the PIN from the smart card.

7. The method according to Claim 6 further comprising:

storing on the on-line authorization system the entity-identifier x and a reference cryptogram $E_{KBD}[y_r]$ where KBD is a database key.

8. The method according to Claim 6 further comprising:

receiving at the smart card the entity-entered PIN′ via an entity-activated terminal;

generating on the smart card a random number a_t between a lower limit L and the large prime integer P;

computing at the smart card a polynomial:

$$y_t = PIN' + \sum_{i=1}^{N} a_{ti} \cdot x^i (\text{mod}\, P);$$

a value:

$a_r' = PIN' \cdot z_r \text{ (mod P)}$; and

a difference $d = a_r' - a_t$;

erasing the random number a_t from the smart card;

encrypting the value y_t and the difference value d at the smart card as encryption function $E_{KC}[d, y_t]$ under a transmission key KC;

sending the encryption function $E_{KC}[d, y_t]$ to the host.

9. The method according to Claim 8 further comprising:

receiving at the host the encryption function $E_{KC}[d, y_t]$; and

verifying the PIN′ is equal to the PIN on condition that:

$d \cdot x = y_r - y_t \text{ (mod P)}$.

10. The method according to Claim 1 wherein:

information sent from the smart card to the host is sufficient to verify the PIN although insufficient for reconstructing the PIN.

11. The method according to Claim 1 wherein:

for an individual account corresponding to the entity-identifier x, the host maintains a single point on a curve represented by a reference polynomial so that the information stored on the host is insufficient to reconstruct the polynomial and recover the PIN.

12. The method according to Claim 1 wherein:

the smart card creates an irreversible form of the entered PIN′ that probabilistically differs on every transaction and probabilistically differs from any reference information on the host.

13. The method according to Claim 1 wherein:

the smart card creates a probabilistically different random and ephemeral polynomial on every transaction and operates on only one point from the polynomial with the polynomial coefficients erased after every usage and restricted from transmission to the host.

14. The method according to Claim 1 wherein:

the Personal Identification Number (PIN) is selected from among members of a group consisting of identification numbers, passwords, biometric data, fingerprints, retinal scans, electrical body signals, and pictorial images.

15. A data security apparatus comprising:

a smart card capable of on-line Personal Identification Number (PIN) verification comprising:

an interface capable of communicating with an on-line authorization system and/or a host;

a processor coupled to the interface; and

a memory coupled to the processor and having a computable readable program code embodied therein that executes enrollment and transaction operations for on-line PIN verification based on hiding an entity-selected PIN in an ephemeral polynomial over a finite field.

16. The apparatus according to Claim 15 wherein the memory further comprises:

a computable readable program code capable of causing the processor to hide the entity-selected PIN in a polynomial over a finite field of the form:

$$y = a_0 + \sum_{i=1}^{n} a_i x^i \pmod{P},$$

where P is a large prime number.

17. The apparatus according to Claim 15 wherein:

the smart card sends information to the host that is sufficient to verify the PIN although insufficient for reconstructing the PIN.

18. The apparatus according to Claim 15 wherein the memory further comprises:

a computable readable program code capable of causing the processor to receive a large prime integer P, an entity-identifier x, and the entity-selected PIN;

a computable readable program code capable of causing the processor to generate on the smart card a random number a_r between a lower limit L and the large prime integer P;

a computable readable program code capable of causing the processor to compute a polynomial:

$$y_r = PIN + \sum_{i=1}^{N} a_{ri} \cdot x^i (\mathrm{mod}\, P);$$

a computable readable program code capable of causing the processor to encrypt value y_r as encryption function $E_k[y_r]$;

a computable readable program code capable of causing the processor to send the encryption function $E_k[y_r]$ to the on-line authorization system;

a computable readable program code capable of causing the processor to compute on the smart card at least one value:

$z_i = PIN^{-1} \cdot a_{ri} (\mathrm{mod}\ P)$;

a computable readable program code capable of causing the processor to retain the at least one value z_i on the smart card; and

a computable readable program code capable of causing the processor to erase the random number a_r and the PIN from the smart card.

19. The apparatus according to Claim 15 wherein the memory further comprises:

a computable readable program code capable of causing the processor to initialize a smart card with an entity-selected PIN hidden in a reference polynomial over a finite field, the reference polynomial being a function of the PIN, an entity-identifier, and a random number;

a computable readable program code capable of causing the processor to send the entity-identifier and a function of the reference polynomial to an on-line authorization system for enrollment;

a computable readable program code capable of causing the processor to retain a secret function of the random number and inverse of the PIN on the smart card; and

a computable readable program code capable of causing the processor to discard the random number and the PIN.

20. The apparatus according to Claim 19 wherein the memory further comprises:

a computable readable program code capable of causing the processor to receive an entity-entered PIN′ via an entity-activated terminal, enabling recovery from a polynomial over a finite field;

a computable readable program code capable of causing the processor to compute an ephemeral transaction polynomial as a function of the entity-entered PIN′, the entity-identifier, and a second random number;

a computable readable program code capable of causing the processor to send to a host a function of the ephemeral transaction polynomial, the host being capable of verifying that PIN is equivalent to PIN′ at the host based on a relationship among the entity-identifier, a function of the reference polynomial, and the function of the ephemeral transaction polynomial; and

a computable readable program code capable of causing the processor to discard the second random number.

21. The apparatus according to Claim 20 wherein:

the smart card creates an irreversible form of the entered PIN′ that probabilistically differs on every transaction and probabilistically differs from any reference information on the host.

22. The apparatus according to Claim 20 wherein:

the smart card creates a probabilistically different random and ephemeral polynomial on every transaction and operates on only one point from the polynomial with the polynomial coefficients erased after every usage and restricted from transmission to the host.

23. The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code capable of causing the processor to encrypt the function of the reference polynomial prior to sending to the on-line authorization system; and

a computable readable program code capable of causing the processor to encrypt the function of the ephemeral transaction polynomial prior to sending to the host.

24. The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code capable of causing the processor to receive the entity-entered PIN′ via an entity-activated terminal;

a computable readable program code capable of causing the processor to generate on the smart card a random number a_t between a lower limit L and the large prime integer P;

a computable readable program code capable of causing the processor to compute at the smart card a polynomial:

$$y_t = PIN' + \sum_{i=1}^{N} a_{ti} \cdot x^i \pmod{P};$$

a value:

$a_r' = PIN' \cdot z_i \pmod{P}$; and

a difference $d = a_r' - a_t$;

a computable readable program code capable of causing the processor to erase the random number a_t from the smart card;

a computable readable program code capable of causing the processor to encrypt the value y_t and the difference d as encryption function $E_{KC}[d, y_t]$ under a transmission key KC;

a computable readable program code capable of causing the processor to send the encryption function $E_{KC}[d, y_t]$ to the host.

25. A data security apparatus comprising:

an enrollment terminal for usage with an on-line host authorization system comprising:

a communication interface capable of communicating with a network, a user interface, and a smart card interface configured to accept a smart card that executes initialization and transaction operations for on-line Personal Identification Number (PIN) verification based on hiding an entity-selected PIN in an ephemeral transaction polynomial over a finite field;

a processor coupled to the communication interface; and

a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to supply to the smart card a modulus P, an entity-identifier x, and a reference Personal Identification Number (PIN) for smart card computation of a reference polynomial of the form:

$$y_r = PIN + \sum_{i=1}^{n} a_{ri} x^i \pmod{P},$$

and having a computable readable program code capable of causing the processor to transfer from the smart card to a host the entity-identifier x and a function of the reference polynomial y_r.

26. The apparatus according to Claim 25 further comprising:
a computable readable program code capable of causing the processor to encrypt the reference polynomial to a reference cryptogram.

27. The apparatus according to Claim 25 wherein:
the smart card sends and the on-line host authorization system stores information that is sufficient to verify the PIN although insufficient for reconstructing the PIN.

28. The apparatus according to Claim 25 wherein:
the on-line host authorization system receives from the smart card an encrypted reference polynomial function.

29. A data security apparatus comprising:
a host system capable of on-line Personal Identification Number (PIN) verification comprising:
a communication interface capable of communicating with a terminal configured to accept a smart card that executes enrollment and transaction operations for on-line PIN verification based on hiding an entity-selected transaction PIN′ in an ephemeral polynomial over a finite field;
a host database capable of storing enrollment information for a plurality of enrolled smart cards;
a processor coupled to the communication interface and the host database; and
a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to receive from a transacting smart card information relating to a point on a curve generated from a polynomial hiding an entered

transaction PIN′ and compare the smart card information to database information relating to a point on a curve generated from a reference polynomial hiding a reference PIN.

30. The apparatus according to Claim 29 wherein the memory further comprises:

a computable readable program code capable of causing the processor to receive an ephemeral transaction polynomial function from the smart card, receive an entity-identifier and reference polynomial function from the host database, and perform a comparison operation verifying that the reference PIN is equivalent to the transaction PIN′ at the host based on a relationship among the entity-identifier, a function of the reference polynomial, and the function of the ephemeral transaction polynomial.

31. The apparatus according to Claim 29 wherein:

neither the host system nor the smart card have sufficient information to reconstruct the entity-selected PIN but do have sufficient information to verify that the correct PIN′ is entered.

32. The apparatus according to Claim 29 wherein:

the reference polynomial function and the ephemeral transaction polynomial function are polynomials of the form:

$$y = a_0 + \sum_{i=1}^{n} a_i x^i \pmod{P},$$

where P is a large prime number.

33. The apparatus according to Claim 29 wherein:

information sent from the smart card to the host system is sufficient to verify the PIN although insufficient for reconstructing the PIN.

34. The apparatus according to Claim 29 wherein:

for an individual account corresponding to the entity-identifier, the host system maintains a single point on a curve represented by a reference polynomial so that the information stored on the host system is insufficient to reconstruct the polynomial and recover the PIN.

35. The apparatus according to Claim 29 wherein:

the smart card creates an irreversible form of an entered PIN that probabilistically differs on every transaction and probabilistically differs from any reference information on the host system.

36. The apparatus according to Claim 29 wherein:

the smart card creates a probabilistically different random and ephemeral polynomial on every transaction and operates on only one point from the polynomial with the polynomial coefficients erased after every usage and restricted from transmission to the host system.

37. A transaction system comprising:

a network;

a plurality of servers and/or hosts coupled to the network;

a plurality of on-line terminals coupled to the servers via the network;

a plurality of smart cards enrolled in the transaction system and capable of insertion into the on-line terminals and performing transactions via the servers; and

a plurality of processors distributed among the smart cards, the servers, and/or the on-line terminals, at least one of the processors being capable of executing enrollment and transaction operations for on-line PIN verification based on hiding an entity-selected PIN in an ephemeral polynomial over a finite field.

38. The transaction system according to Claim 37 wherein at least one of the processors can execute a method for on-line Personal Identification Number (PIN) verification comprising:

initializing a smart card with an entity-selected PIN hidden in a polynomial over a finite field, a reference polynomial being a function of the PIN, an entity-identifier, and a random number; and

discarding the random number and the PIN after smart card initialization.

39. The transaction system according to Claim 38 wherein the method for on-line Personal Identification Number (PIN) verification further comprises:

generating an ephemeral transaction polynomial using the smart card at an entity-activated terminal with an entity-entered PIN′ enabling recovery from a polynomial over a finite field, the ephemeral transaction polynomial being a function of the entity-entered PIN′, the entity-identifier, and a second random number;

sending a function of the ephemeral transaction polynomial and the difference between the second random number and a function of the PIN′ and the secret function to a host; and

discarding the second random number.

40. The transaction system according to Claim 39 wherein the method for on-line Personal Identification Number (PIN) verification further comprises:

verifying that the reference PIN is equivalent to the transaction PIN′ at the host based on a relationship among the entity-identifier, a function of the reference polynomial, and the function of the ephemeral transaction polynomial.

41. A transaction system comprising:

means for verifying a Personal Identification Number (PIN);

means for initializing a smart card with an entity-selected PIN hidden in a polynomial over a finite field, a reference polynomial being a function of the PIN, an entity-identifier, and a random number;

means for sending the entity-identifier and a function of the reference polynomial to an on-line authorization system for enrollment;

means for retaining a secret function of the random number and inverse of the PIN on the smart card; and

means for discarding the random number and the PIN.